Policy Title: Payment Card Industry Data Security Standard (PCI-DSS) Requirements
Policy Summary: University Policy for Processing Payment Card Activities in Accordance with Payment Card Industry Data Security Standard Requirements
Policy Category: Financial
Policy Owner: Finance

Policy Summary

All employees that accept, process, handle, transmit or dispose payment card (credit or debit cards) information are required to abide by Payment Card Industry (PCI) Data Security Standards (DSS) and take applicable training.

Purpose

Drake University is obligated to abide by PCI-DSS that mandate how payment card data is stored, transmitted and secured. The PCI-DSS also requires those coming into contact with PCI data to take training about the standard and the importance of security.

This document establishes roles, responsibilities, and rules for card processing activities, enabling the university to maintain compliance with the PCI-DSS while safeguarding customer payment card data.

Scope

This policy governs payment card acceptance, processing, handling, transmission, and disposal by all departments and individuals at all locations on behalf of Drake University. This includes card-present and card-not-present transactions on physical card readers, via the internet on University-managed e-commerce websites, or via third-party vendors.

Definitions

Card processing owner: Individual responsible for payment card processing in a specific department, college, school, etc., ("Department") or a specific merchant ID.

Cardholder data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

PAN: Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Payment Card Industry Data Security Standard (PCI-DSS): The security requirements defined by the Payment Card Industry Security Standards Council and the five major Payment Card brands: Visa, MasterCard, American Express, Discover, JCB. Any organization accepting, processing, transmitting, or storing payment card information is contractually bound to adhere.

Attestation of Compliance (AoC): The form for merchants and service providers to attest to the results of a PCI-DSS assessment, demonstrating compliance.

Confidential Information: Information determined to require the highest level of privacy and security controls, including information regulated by federal or state laws or industry regulations.

Acquiring Bank: Merchant bank contracted through Finance on behalf of all departments and affiliates to perform banking and card processing services.

Responsibility

1. All members of the University community share the responsibility for protecting information and data with which they are entrusted. Departments that manage Payment Card transactions must adhere to the strict requirements of this policy and of the PCI-DSS.
2. All cardholder data is classified as Confidential, Level 1 as outlined in Drake Information Security Policy.
3. Access to payment card processing systems and information must be restricted to appropriate personnel. It is the responsibility of each department's card processing owner to ensure that all personnel involved in payment card transactions understand all requirements outlined in this document.
4. All individuals who accept, process, handle, transmit, support, or manage payment card transactions must complete PCI training upon hire and annually thereafter. The Controller's Office and Information Security & Compliance will assign and facilitate training.
5. Third parties providing payment gateways or processing services must provide an Attestation of Compliance annually.

Card Processing Personnel

1. Report data breach incidents in a timely fashion, following all existing policy and procedure. See Data Security Breach Response below under Policy for more information.
2. Cooperate with Finance and Information Security initiatives to improve risk posture and abide by PCI-DSS requirements.
3. Complete training and acknowledge requirements upon hire and at least annually thereafter, including Drake University and PCI-DSS requirements for cardholder data security.
4. Follow all requirements of the PCI-DSS.

Card Processing Owners

1. Provide information about specific payment card handling intentions, procedures, and practices when requested.
2. Maintain a current list of departmental card processing personnel, notifying the Controller's Office when changes occur and annually.
3. Report data breach incidents in a timely fashion, following all existing policy and procedure. See Data Security Breach Response below under Policy for more information.
4. Cooperate with Finance and Information Security initiatives to improve risk posture or abide by PCI-DSS requirements.

5. Complete training and acknowledge requirements upon hire and at least annually thereafter, including Drake University and PCI-DSS requirements for cardholder data security.
6. Ensure all departmental card processing personnel complete assigned training. If training is not completed, the merchant number may be deactivated.
7. Follow all requirements of the PCI-DSS.

Controller's Office

1. Maintain ownership of all University merchant IDs in use.
2. Provide oversight over all processing of payment cards.
3. Create and maintain merchant ID instances based on usage, volume, and business need.
4. Assist with PCI-DSS attestation and enforcement.
5. Assist with data breach response.
6. Review and update this document as appropriate.

Information Security & Compliance

1. Maintain overview responsibility for implementation of technical requirements in this document as well as overall PCI-DSS requirements.
2. Mandate requirements that conform to PCI-DSS standards for payment card processing.
3. Assist with PCI-DSS attestation and enforcement.
4. Assist with data breach response.
5. Review and update this document as appropriate.

Policy

Card Acceptance

1. In the course of conducting University business, it may be necessary for certain departments to accept payment cards. The creation of a new merchant ID for the purpose of accepting and processing payment cards at the University is done on a case by case basis and **must be** coordinated through the Controller's Office. Any fees associated with the acceptance of payment cards, including the cost of equipment and transaction fees, will be charged to the requesting department.
2. Any department accepting payment cards on behalf of the University must designate a card processing owner within the department who will have primary authority and responsibility within that department for card transactions.
3. Third party service providers must complete and return a Vendor Risk Assessment Questionnaire, available through ITS Project Management or Information Security & Compliance, prior to formal contract signature and any data processing, transmission, or storage.
4. Contracts with third party service providers approved by the Controller's office must state their adherence to and compliance with the PCI-DSS and attest to that compliance annually.
5. To comply with contractual obligations, all departments must use Drake University's acquiring bank to perform all card processing services.

Payment Card Security

Every card processing owner must have in place and/or abide by the following components and ensure that these components are maintained on an ongoing basis.

1. Payment card data may not be stored electronically for any reason on any system, including University-issued and personal computers and electronic media devices, including, but not limited to, the following: desktops, laptops, CDs, DVDs, USB flash drives, portal hard drives, smartphones, tablets, or PDAs.
2. Payment card processing is restricted only to those with a specific business need or requirement as part of their job description and duties and have undergone information security training on the handling of cardholder data.
3. Cardholder data stored on paper must be protected against unauthorized access and destroyed by crosscut shredding as soon as the data is no longer needed.
4. All equipment used to collect data must be secured against unauthorized use.
5. Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment used to process cardholder data and any documents containing cardholder data.
6. Compliance is a joint effort. The Controller's Office and Information Security & Compliance will work jointly with all departments that process payment cards to ensure that the departments are compliant with PCI-DSS requirements. Individual departments are held responsible for PCI compliance for all departmental procedures, applications, point of sale devices and departmentally administered systems that process and/or transmit cardholder data.
7. Messaging technologies such as email, instant messaging, social media, or other University or cloud-hosted services and systems must not be used to transmit or store cardholder data, nor should it be used as a method to supply such information. If it does occur, Information Security & Compliance must be notified.

Data Security Breach Response

If a breach of security is suspected or confirmed in any department's payment card processing environment, the relevant card processing owner and/or personnel in areas that process payment cards must follow University Security Policy 1.6 - Reporting Electronic Security Incidents immediately. In short:

1. Notify ITS personnel of the suspected or confirmed breach by contacting the ITS Support Center at (515) 271-3001, a member of the Information Security & Compliance team at informationsecurity@drake.edu, or any member of the ITS administration team.
2. Disconnect the device(s) from the network *only* by removing the network cable or disabling the wireless network card. Do not modify the power state of the device.
3. Document all actions taken from the point of the discovery of suspected breach, preserving any evidence available.
4. Notify the Controller's Office of the merchant ID most closely associated with the incident.
5. Do not disclose details of the suspected breach by email, other than initial notification.
6. Secure any device(s) on which a breach of security is suspected by preventing others from accessing the device, in order to preserve evidence.
7. Information Security & Compliance and the Controller's Office will form an Incident Response team to determine next steps and respond in accordance with compliance obligations.

Compliance

1. Failure to comply with PCI-DSS requirements may result in suspension of payment processing privileges for the affected department.
2. The PCI-DSS requirements exist to protect cardholders and their information, and violations may incur monetary fines regulatory infractions from regulatory bodies. The Controller's Office may recoup these costs from the non-compliant department.

Resources and Related University Policies:

- Vendor Risk Assessment Questionnaire
- Information Technology Services policies:
    - Information Security
    - Reporting Electronic Security Incidents